PCT/DE98/01922

Patent claims

Sub a1

1. A method for mutual authentication of components in a network using the challenge-response method, in which, in order to authenticate a terminal (M), in particular a mobile station, with the network, the network (N) uses a request to request from an authentication center (AUC) at least one data pair comprising a first random number (Challenge 1) and a first response (Response 1), and passes the first random number (Challenge 1) to the terminal (M) which uses an internally stored key (Ki) likewise to calculate from this the first response (Response 1) and sends this to the network (N), in which case, furthermore, the network (N) is authenticated with the terminal (M) in that the terminal sends a second random number (Challenge 2) to the network, to which the network responds with a second response (Response 2) calculated in the AUC,

wherein

the first response (Response 1) sent from the terminal (M) to the network (N) is at the same time used as the second random number (Challenge 2), in which case the network has already requested the second response (Response 2) from the AUC in advance, together with the

Article 34 Amd't

first random number and the first response, as part of a triplet data set (Challenge 1/Response 1/Response 2).

2. The method as claimed in claim 1, wherein the network interprets the first response (Response 1), which is sent back from the terminal (M), as the second random number (Challenge 2).

AMENDED SHEET

Article 34 Amdt

3. The method as claimed in claim 1 or 2, wherein the first random number (Challenge 1) and the first response (Response 2) are transmitted from the network (N) to the terminal (M) immediately successively in time.

4. The method as claimed in claim 1 or 2, wherein the data pair (Challenge 1/Response 2) is transmitted from the network (N) to the terminal (M) simultaneously, in the form of a single data set.

5. The method as claimed in one of claims 2, 3 or 4, wherein the network requests data sets from the authentication center (AUC) in the form of triplet data sets (Challenge 1/Response 1/Response 2).

6. The method as claimed in claim 5, wherein a plurality of triplet data sets are supplied from the AUC as a stockpile, in order to reduce the request frequency.

7. The method as claimed in claim 4 or 5, wherein, in order to use the first response (Response 1) of the terminal (M) as the second random number (Challenge 2) in order to authenticate the network with the terminal (M), the shorter length of the first response (Response 1) is filled out to make up the greater length of the second random number (Challenge 2).

AMENDED SHEET

Article 34 Amdt

8. The method as claimed in claim 7, wherein the filling-out process is carried out on a subscriber-specific basis, and wherein the complete length of the first response (Response 1) is shortened before transmission to the other station.

9. The method as claimed in claim 8, wherein the first response (Response 1) is filled out with defined bits from the

09462916.040300

AMENDED SHEET

secret key (Ki) to make up the length of the second random number (Challenge 2).

10. The method as claimed in claim 8, wherein the second random number (Challenge) corresponds to the original first response (Response 1) before it was shortened.

11. The method as claimed in one of claims 1-10, wherein the network is a GSM network.

12. The method as claimed in one of claims 1-10, wherein the network is a wire-based network.

13. The method as claimed in claim 12, wherein the individual, mutually authenticating components in a wire-based network are different monitoring units of computers which authenticate themselves with a central computer, and vice versa.

14. The method as claimed in one of claims 1-13, wherein the AUC calculates the triplet data sets requested by the network and transmits these to the network off-line and independently of time, on request by the network, but in any case before the data interchange between the network and the terminal.